SISEMINISTEERIUM

Justiits- ja Digiministeerium

Teie: 02.05.2025 nr 17.1.1/25-0207/-2T

Meie: 28.05.2025 nr 5-1/23-2

Siseministeeriumi arvamus Euroopa Liidu küberturvalisuse määruse avaliku konsultatsiooni kohta

Tulenevalt Riigikantselei resolutsioonist 4-2/25-00837 edastab Siseministeerium arvamuse Justiits- ja Digiministeeriumile seoses Euroopa Liidu (edaspidi *EL*) küberturvalisuse määruse avaliku konsultatsiooniga. Ülevaate koostasid Siseministeeriumi EL ja välissuhete osakond, sisejulgeoleku osakond ning digi- ja teabehaldusosakond. Valdkondade eest vastutab Siseministeeriumi kantsler Tarmo Miilits (tarmo.miilits@siseministeerium.ee).

Siseministeerium tervitab võimalikku määruse eelnõu koostamist tulevikus ning toetab kogu valdkonna avamist pilguga, mis tänapäeva keerulises, konfliktiohtude kasvavas õhustikus suudaks pakkuda paindlikku, kiiret ja arengukiirusega kaasaskäivaid lahendusi. Kui tehnoloogia edeneb tohutu kiirusega, siis selle kasutust kaitsev turve ning seda omakorda toetav protsess peab muutuma samuti: paindlikuks, fokusseeritumaks ja sektoripõhisust enam arvestavamaks.

Avalikus konsultatsioonis pakutud poliitikavariantide vahel valimine on keerukas, kuna kõigi esitatud valikutega saab seatud eesmärke saavutada teatud määral, kuid mitte tingimata maksimaalselt. Seetõttu on oluline hinnata iga poliitikavariandi mõju ulatust ja praktilist teostatavust, lähtudes nii küberturvalisuse taseme tõstmisest kui ka halduskoormuse mõistlikust vähendamisest. Keskseks küsimuseks peaks olema, millise lahenduse abil on võimalik tagada eesmärkide võimalikult tõhus täitmine, säilitades samal ajal nii õigusliku selguse kui ka kohaldamise lihtsuse. Seejuures tuleks vältida ülereguleerimist ning eelistada paindlikke lahendusi, mis arvestavad kiiresti muutuva tehnoloogiakeskkonna ja küberohtude dünaamikaga.

Küberturvalisuse tagamine on olemuslikult keeruline, ressursimahukas ja pidevas arengus. Küberturvalisuse tagamine nõuab, et kasutatavad meetmed oleksid piisavalt tugevad, et pakkuda kaitset, kuid samas piisavalt paindlikud, et mitte seada takistusi innovatsioonile ega aeglustada tehnoloogilist arengut. Regulatsioonid peaksid seega looma keskkonna, kus turvalisus ja areng ei ole omavahel vastuolus, vaid teineteist toetavad.

Sellest tulenevalt esitab Siseministeerium mõned sisulised kommentaarid:

1. Regulatiivset raamistikku tuleks hinnata tervikuna, eesmärgiga vältida olukorda, kus olemasolevad normid ja menetlused muutuvad ajamahukaks, bürokraatlikuks ja pärsivad kiiret

reageerimist uutele ohtudele või tehnoloogilistele muutustele. Valdkonnas, kus ajafaktor on sageli määrava tähtsusega, peab regulatsioon toetama „võidujooksu“ ründajate ja nende kasutatavate tehnoloogiate vastu, mitte pidurdama seda.

2. Olulist tähelepanu tuleks pöörata kohustuste lihtsustamisele, kus see on mõistlik ja teostatav – sealhulgas aruandluse, sertifitseerimise ning auditeerimise osas. Lihtsustamine peaks põhinema põhimõttel, et vähem bürokraatiat tähendab suuremat tõhusust. Samal ajal tuleks säilitada selgus ja läbipaistvus, et tagada süsteemi usaldusväärsus. Kaaluda võiks standardiseeritud nõudeid või sektorite üleseid raamistikke, et vältida killustatust ning toetada piiriülest koordineeritust.

3. Vajalik on kriitiliselt üle vaadata regulatiivsete nõuete rakendatavus erinevates sektorites, sh hinnata, kas seatud nõuded ja ootused on ühetaoliselt kohaldatavad nii suurtele kui ka väikestele ettevõtetele, avalikule kui ka erasektorile, samuti erinevat tüüpi taristule (tavataristu, kriitiline taristu, elutähtis teenus). Olukorras, kus eri sektorid või turuosalised on väga erineva suuruse, riskitaseme või ressursivõimekusega, tuleks kaaluda selgete ja põhjendatud erisuste kehtestamist, et tagada nõuete proportsionaalsus.

4. Auditeerimise ja sertifitseerimise ajavahemikud tuleks kriitiliselt üle vaadata, et need ei muutuks innovatsiooni ja arendustegevust pärssivaks takistuseks. Kaitsemeetmed peavad suutma areneda samas tempos ohtude ja tehnoloogilised lahenduste arenguga. Seega peaks auditeerimise sagedus ja ulatus põhinema riskihinnangul ning süsteemide olulisusel, mitte pelgalt formaalsetel tsüklitel. Eesmärgiks peaks olema dünaamiline ja kohanduv järelevalveraamistik, mis soodustab turvalisust, mitte selle stagnatsiooni.

5. Väärib tähelepanu ka see, millised on nõuded auditeerijatele ja sertifitseerijatele. Kuigi sõltumatus ja usaldusväärsus on hindamatud, ei tohiks kontrollimehhanismid muutuda liigselt formaalseks ega keskenduda pelgalt bürokraatlikele detailidele. Auditeerimise väärtus seisneb selles, kuidas see aitab kaasa auditeeritava organisatsiooni sisemisele arengule ja turvalisuse kasvule, mitte pelgalt linnukese saamisele. Ehk rõhuasetus peab olema auditeeritavate toetamisel, nõustamisel ja suunamisel.

6. Erilist tähelepanu vajab koordineeritus teiste EL-i regulatsioonidega, et vältida paralleelsete ja kattuvate nõuete tekkimist. Küberturvalisuse määrust tuleks käsitleda osana laiemast EL-i õigusraamistikust. Eesmärgiks peab olema nõuete kooskõla ja sellise olukorra vältimine, kus organisatsioon peab vastama mitmele erinevale, ent sisult samale kohustusele.

7. Tuleks edendada EL-i ülest koolitus- ja teavitusraamistikku, mis toetaks regulatiivsete nõuete ühtset mõistmist ja rakendamist. Sertifitseerimise ja turbenõuete edukas elluviimine eeldab pädevusi ja teadlikkust, mida ei saa automaatselt eeldada kõikidelt subjektidelt.

8. Arvesse tuleks võtta EL-i küberturvalisuse ökosüsteemi kui terviku küpsusastet, sh erinevate liikmesriikide arengutaset ja suutlikkust regulatiivseid muudatusi rakendada. Tasakaalu leidmine ambitsioonikate eesmärkide ja liikmesriikide tegelike rakendusvõimekuste vahel on hädavajalik.

Lugupidamisega

(allkirjastatud digitaalselt)

Tarmo Miilits
kantsler

Katarina Budrik 6125144
katarina.budrik@siseministeerium.ee